INDIALAW

CIVIL

Strengthening Cybersecurity: MCX Updates SOP for Handling Cybersecurity Incidents

AUTHOR Rahul Sundaram

PUBLISHED 10 January 2025

The Multi Commodity Exchange of India Limited (MCX) has issued a revised Standard Operating Procedure (SOP) for managing cybersecurity incidents vide a circular dated January 8,2025. This updated SOP aligns with the Securities and Exchange Board of India (SEBI)'s Cybersecurity and Cyber Resilience Framework (CSCRF) as outlined in the SEBI circular dated August 20, 2024. It sets clear directives and timelines for incident reporting and management, aiming to bolster the security framework for regulated entities (REs), members, and depository participants (DPs).

Table of contents

Background and Objective

Cybersecurity threats have been a growing concern for financial markets globally, and the revised SOP by MCX is a proactive step to mitigate these risks. The framework updates prior guidelines issued in 2021 and reflects the latest SEBI circular requirements. The SOP emphasizes timely reporting, stringent mitigation measures, and detailed post-incident evaluations to ensure that all stakeholders follow a robust and unified approach to managing cybersecurity incidents.

The SOP aims to protect trading networks, prevent lateral threat movements, and enhance the overall cyber resilience of SEBI-regulated entities.

Key Provisions of the SOP

1. **Mandatory Incident Reporting**:
   - REs, members, and DPs must report cybersecurity incidents within **6 hours** of detection or notification. This ensures swift containment and limits potential damage.
   - In cases where submission through SEBI or exchange portals is not possible, entities can report via email to designated group IDs.
2. **Classification and Containment**:
   - Incidents are classified into Critical, High, Medium, and Low categories based on severity.
   - For incidents classified as Critical or High, connectivity between affected entities and exchanges/depositories may be disabled until a certified report confirms risk mitigation.
3. **Post-Incident Submissions**:
   - Entities must submit various reports, including immediate, interim, and root cause analysis (RCA) reports, within stipulated timelines.

Timelines for Post-Incident Reporting

MCX has established the following timelines to ensure the prompt and structured handling of cybersecurity incidents:

Immediate Cyber Incident Reporting	Within **6 hours**
Immediate Mitigation Measure Report	**Same day**
Interim Report	**T + 3 Days**
Mitigation Measure Report	**T + 7 Days**
Root Cause Analysis (RCA) Report	**T + 30 Days** (extensions in special cases)
Forensic Audit Report (if required)	**Maximum 75 Days**

Vulnerability Assessment & Penetration Testing (VAPT) Report	**T + 45 Days**

(*T refers to the date of detection or notification of the incident.*)

Compliance and Penalty Framework

Failure to adhere to the specified timelines could result in penalties. For instance, delays in reporting incidents, submitting RCA reports, or forensic audit findings could attract fines of up to ?10 lakhs per incident for larger entities. Repeat or significant non-compliance could lead to trading restrictions or suspension of connectivity.

Conclusion

The updated SOP reflects the increasing importance of cybersecurity in protecting financial markets. By setting stringent timelines and detailed reporting protocols, MCX aims to ensure rapid incident resolution and minimize disruptions. This framework underscores the commitment of market infrastructure institutions to maintaining robust cyber defenses while fostering trust among stakeholders. It is now imperative for regulated entities to fully comply with the SOP to avoid penalties and contribute to the resilience of India’s financial ecosystem.

With the implementation of this SOP from January 20, 2025, MCX and its participants take a significant step forward in strengthening the cybersecurity posture of the Indian financial markets.